IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, v. MOHAMMED AZHARUDDIN CHHIPA, *Defendant*.	Case No.: 1:23-cr-97 (DJN)

DEFENDANT'S REPLY ON HIS MOTION TO SUPPRESS THE CONTENT OF UNLAWFUL ELECTRONIC SURVEILLANCE AND FRUIT THEREOF, AND TO COMPEL DISCLOSURE OF ALL SURVEILLANCE MATERIAL

The government's opposition faults Mohammed Chhipa for not articulating specifics against factual allegations he cannot see, and not adequately countering arguments he is prohibited from knowing. *See generally Gov't Unclassified Resp. in Opp. to Def.'s FISA Mot.*, ECF No. 124 (Aug. 30, 2024). For example, the government chides the defense for raising merely a "theoretical impropriety," (at 38) and argues that the defense has failed to "flag issues" where counsel's input would be "necessary" (at 44).

That Mr. Chhipa was actually able to assert more than a "theoretical impropriety," and flag concrete issues where counsel's input would be necessary in his FISA Motion to Suppress (ECF No. 111) is nothing short of remarkable given

that cleared defense counsel is required to draft this motion essentially blindfolded by *ex parte* proceedings that contain the entirety of the substantive material.

Argument

More than "theoretical" impropriety

The impropriety asserted by Mr. Chhipa as it relates to the FISA process far from theoretical. Mr. Chhipa detailed numerous instances of FISA and Fourth Amendment compliance issues by the FBI. *See* ECF No. 111 at 42-48. According to the independent Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702* at 143 (Sept. 28, 2023) ("PCLOB 2023 Report").[1] "FBI's reported compliance incidents have numbered in the thousands or tens of thousands, depending on the year… In 2022, the government suspended reporting this rate…."

The Foreign Intelligence Surveillance Court has repeatedly opined on these as well, year after year.

- 2018 – a FISC opinion explained that the FBI's procedures "as they have been implemented, are not consistent with the requirements of Section 1801 (h)(1) and (h)(3), or the Fourth Amendment." *Redacted*, 402 F. Supp. 3d 45, 82 (Foreign Intel. Surv. Ct. 2018), aff'd in part sub nom. *In re DNI/AG 702(h) Certifications 2018*, 941 F.3d 547 (Foreign Int. Surv. Ct. Rev. 2019).

- 2019 – a FISC opinion found "material misstatements and omissions in the [FISA] applications filed by the government." *In re Accuracy Concerns Regarding FBI Matters Submitted to FISC*, 411 F. Supp. 3d 333, 334–35 (Foreign Intel. Surv. Ct. 2019). It detailed misrepresentations in FISA warrant applications made by the FBI; specifically that the FBI made representations that were "unsupported or contradicted by information in

[1] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

their possession," and "withheld information detrimental to their case." *Id.* at 337. This conduct, the FISC explained, was "antithetical to the heightened duty of candor" necessary in the *ex parte* context. *Id.* More broadly, the FISC stated that this issue "calls into question whether information contained in other FBI applications is reliable." *Id.*

- 2020 – a FISC opinion described "widespread violations" by the FBI. *FISC Opinion*, Nov. 18, 2020 at 39.[2]

- 2021 – the opening line of a FISC opinion refers to the FBI's "compliance problems," (at 1) and later discusses violations numbering in the tens of thousands (at 150-151). *FISC Order In Response to Querying Violations* (Sept. 2, 2021).[3] That same opinion calls the FBI's violation "substantial and persistent," and states that a "[f]ailure to correct them would call into question the continued validity, as implemented, of the FBI SMPs for Title I and Title Ill and the FBI BR SMPs, as well as the ability of a FISC judge to find the FBI's Section 702 procedures, as implemented, to be consistent with statutory and Fourth Amendment requirements." *Id.* at 13-14.

- 2022 – yet another FISC opinion reports "additional, significant violations" (at 28) and characterized compliance problems "persistent and widespread" (at 49). *FISC Memorandum Opinion and Order*, April 21, 2022.[4]

Order after order, going at least as far back as 2018, details the FISC's continued frustrations with the FBI's violations, which it acknowledges in some instances run afoul of the Fourth Amendment and call into question the reliability of the entire process. These opinions and findings make clear that Mr. Chhipa's concern of impropriety is hardly "theoretical" but, in fact, well documented.

[2]https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf
[3]https://www.intel.gov/assets/documents/702%20Documents/declassified/21/FISC_Sept2_2021_Order_In_Response_To_Querying_Violations.pdf
[4]https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf

Ex parte Franks issues

The government represents that there are no *Franks* issues and that Mr. Chhipa should simply accept the government at its word with a judicial blessing. *See* ECF No. 124 at 37. That is not how our adversarial system functions. In fact, the misrepresentations outlined in the prior section were not revealed until additional oversight was involved, even with a court (FISC) overseeing the procedures. "[M]ost of FBI's compliance incidents have been discovered through audits by oversight entities rather than through internal compliance review." PCLOB 2023 Report at 119. If an opposing side is present, the revelations will be even more significant, as explained in *United States v. James Daniel Good Real Property, et. al.*, 510 U.S. 43, at 55 (1993): "Fairness can rarely be obtained by secret, one-sided determination of facts decisive of rights. No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it." (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring).

"[T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." *American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1069 (9th Cir. 1995). Even relying on court involvement would not cure these fatal defects. As Mr. Chhipa noted in his original Motion, the *Carpenter* surveillance had been routinely approved by district courts. It was not until extensive adversarial briefing

that the Supreme Court held that a search warrant was required. *See* ECF No. 111 at 87 (citing *Carpenter v. United States*, 138 S. Ct. 2206 (2018)).

Mr. Chhipa's requests to see the processes used to collect evidence against him conform to the basic, fundamental principle of the adversarial process. In response, the government broadly invokes national security. *See* ECF No. 124 at 44, 50, 54; ECF No. 124-1. The utterance of national security is meant to suspend all notions of otherwise essential tenants of a fair and just system. This position is antithetical to our Constitution. *See e.g. New York Times Co. v. United States*, 403 U.S. 713, 719 (1971)(Black, J. and Douglas, J. concurring) ("The word 'security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law… Secrecy in government is fundamentally anti-democratic[.]"); *United States v. Rosen*, 445 F. Supp. 2d 602, 632 (E.D. Va. 2006), amended, No. 1:05CR225, 2006 WL 5049154 (E.D. Va. Aug. 16, 2006), and aff'd, 557 F.3d 192 (4th Cir. 2009) ("invocation of 'national security' does not free Congress from the restraints of the First Amendment[.]")

Other surveillance and uses of that material

Finally, the government argues that Mr. Chhipa has no standing to assert a Section 702 challenge, and is not entitled to know of any other surveillance techniques used. *See* ECF No. 124 at 42-52. The government correctly explains that an "aggrieved person" is a person who is either the target of electronic surveillance or one whose communications or activities were subject to electronic surveillance. *Id.* at 42 (citing §§ 180l(k), 1881e(a)). The government then goes on to state that

"only an 'aggrieved person' can challenge the electronic surveillance." *Id.* at 43. This is where the government's argument ends. It does not go on to state that Mr. Chhipa is *not* an "aggrieved person." In fact, the most logical inference born of the government's omission is that Mr. Chhipa *is* an "aggrieved person" under the definition in this statute. Therefore, he, in fact, does have standing to challenge the Section 702 surveillance against him.

The government then responds by arguing that it will not "use" any Section 702 material or other surveillance material. Specifically, the government states, "[h]ere, the Government only intends to use *as evidence* against Chhipa information to which he is an aggrieved person that was obtained or derived from electronic surveillance and physical search conducted pursuant to Title I and III of FISA. Accordingly, the Government complied with its notice obligations when it gave notice of its intent to use information obtained or derived from Title I and Title III of FISA." *Id.* at 47. However, the government's constricted view of what constitutes "use" of collected material is error. It ignores the myriad of "uses" of unlawful surveillance that do not necessarily constitute "evidence;" primarily derivative use. "Use" of material does not simply mean material that will be used as evidence at trial.

"[T]he exclusionary rule … reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.'" *United States v. DeQuasie*, 373 F.3d 509, 519 (4th Cir. 2004)(cleaned up); *see also United States v.*

Hernandez, 279 F.3d 302 (5th Cir. 2002) (prior illegal "squeezing" of defendant's luggage while in luggage compartment of bus, although unknown to defendant, taints subsequent consent because the officer "became sufficiently suspicious to engage [defendant] in conversation" in order to obtain consent to a full search of the luggage); *United States v. Politano*, 491 F. Supp. 456, 463 (W.D.N.Y. 1980) ("[T]he request by Agent [] to see the money could only be based upon the information obtained through the prior illegal search at the airport checkpoint by the security personnel and the Cheektowaga police officer."); LaFave, Wayne R., *Search and Seizure: A Treatise on the Fourth Amendment*, § 8.2(d) (5th ed.) (noting that exploitation of a Fourth Amendment violation "may occur by the police taking advantage of earlier illegal acts which are unknown to the consenting party and thus could not have had a coercive effect upon him").

Law enforcement cannot make an initial discovery, for example, gain knowledge of an account through illegal means, and then argue that it does not "use" the material simply because that specific material will not be "evidence." As the Fourth Circuit explained in *United States v. Gaines*, 668 F.3d 170, 175 (4th Cir. 2012), "for purposes of the attenuation doctrine, the *discovery* of the evidence is the relevant event." (citing *Wong Sun v. United States*, 371 U.S. 471, 488, 487) (describing an exception to the exclusionary rule where "the connection between the lawless conduct of the police and the *discovery* of the challenged evidence has become so attenuated as to dissipate the taint") (emphasis added) (internal quotation marks and citation omitted); *United States v. Clark*, 891 F.2d 501, 505

(4th Cir.1989) ("evidence challenged on a suppression motion will not be excluded unless a causal relationship exists between that particular [Fourth Amendment] violation and the *discovery* of the evidence sought to be excluded") (emphasis added); *United States v. Reed*, 349 F.3d 457, 464 (7th Cir.2003) ("The type of intervening events that serve to attenuate [police] misconduct are those that sever the causal connection between the illegal arrest and the *discovery* of the evidence.") (emphasis added); *see also United States v. Coleman*, 536 F. Supp. 3d 80, 84 (S.D.W. Va. 2021) ("a magistrate must know something about the source of information before relying on it to find that probable cause exists.").

Simply the knowledge itself, for example, the unlawful discovery of which accounts to direct legal process, taints any material that flows from it. This reasoning applies whether the discovery is of an account, person, or a house. For example, law enforcement could not illicitly install a hidden camera in a person's home, learn from that footage that the occupant has a sister in whom he confides, serve a grand jury subpoena on that sister, and be able to use her information as evidence. Moreover, law enforcement is prohibited from even using derivative evidence gained from further investigation of her information. The knowledge of where to direct that grand jury subpoena was gathered unlawfully; as such, any material that flows from it is also fatally poisoned.

This reasoning applies even if the unlawfully acquired knowledge is of a public-facing social media account. There are billions of public social media

accounts.[5] Perhaps the largest of the proverbial haystacks in which to find a needle. Conducting an unlawful search to know which one of these billions of accounts to target with legal process is still a fruit of that initial unlawful search. Using the prior example, there are billions of people on the earth roaming about in public, talking in public, driving in public, and entering their homes in public. Conducting an unlawful search to know who, among those in the community, to serve with a grand jury subpoena taints all the information that flows from it. *See United States v. Finucan*, 708 F.2d 838, 844 (1st Cir. 1983) ("Absent the illegal search, the investigators might not have known the identity of all of the third parties nor what to ask them."); *United States v. Cales*, 493 F.2d 1215, 1216 (9th Cir. 1974) (relevant question is whether "anything seized illegally, or *any leads gained from illegal activity*, tend[ed] significantly to direct the investigation toward the specific evidence sought to be suppressed.")(emphasis added).

In this case, it was either Section 702 material, other surveillance, some other type of warrantless search, or varying combinations of all three that formed the basis for the *discovery* of additional evidence, which then may be used against

[5] According to the latest data, there are 5.17 billion social media *users* around the world at the start of July 2024. *See* DataReportal, *Global Social Media Statistics*, https://datareportal.com/social-media-users; *see also* Belle Wong, Top Social Media Statistics And Trends Of 2024, Forbes (May 18, 2023) (https://www.forbes.com/advisor/business/social-media-statistics/)("In 2023, an estimated 4.9 billion people use social media across the world."). If some of these users have multiple accounts, as many do, the number of *accounts* is likely double or triple that figure.

Mr. Chhipa at trial.[6] Defense Exhibits 1 through 3 show that at least as far back as 2013 the FBI had identified nine of Mr. Chhipa's usernames, seven of his email addresses, and three of his phone numbers. The FBI knew of the contacts in Mr. Chhipa's phone, who he called, when, and for how long, and in 2015, the FBI had been evaluating Mr. Chhipa's call patterns for the past two years.

According to the FBI, in the legal processes defense counsel has been permitted to see, the "re-opened" case against Mr. Chhipa was initiated by the FBI "observing" a Carl Johnson Facebook account in 2019. *See e.g.* Def. Ex. 4, *Search Warrant of House* at 3-4 (Aug. 2, 2019). How the FBI even knew to observe this account is the fruit of unlawful searches conducted on Mr. Chhipa before 2019. The defense exhibits show that at least as far back as 2013 the government warrantlessly searched Mr. Chhipa's personal data to reveal identifiers, conversations, calls, contacts, and a host of other information.

This personal information includes the Carl Johnson Facebook account. Thus, when the government states that its case began when it observed the Carl Johnson account in 2019, something triggered that observation of that account. That triggering event – whatever occurred to prompt the FBI to go look for and begin observing the Carl Johnson account – is where the analysis must begin. Any material that follows, including any observation or legal processes, is derived from

[6] Mr. Chhipa must cover all bases since he prohibited from knowing the truth and full extent of the source of the material derivatively used against him. In that regard, he will be filing a separate motion requesting that the Court suppress the fruits of all unlawful searches more generally.

that initial origin. *See United States v. Cordero-Rosario*, 786 F.3d 64, 77 (1st Cir. 2015) (finding relevant "whether absent the illegal search, the investigators would have known the identity of all of the third parties or what to ask them.") (citation and quotations omitted).

In *United States v. Finucan*, 708 F.2d at 843, even though there was no clean, direct link from the unlawful search to obtaining evidence, the court of appeals still affirmed the district court's suppression of evidence. The court found that "the government impermissibly exploited the illegally seized material in gathering some of the additional evidence" because law enforcement may have relied on unlawfully seized documents "in deciding whom to interview and what to ask, and that the documents were taken to the interviews." *Id.*

In this case, there are concrete examples of derivative use of what is likely surveillance material. *First,* as of at least 2013, according to Defense Exhibit 1, the FBI already knew that the Carl Johnson Facebook account was linked to Mr. Chhipa. Yet the first search warrant in this case describes in an incredible way, how the FBI connected the dots between the Carl Johnson account and Mohammed Chhipa. It states:

Def.'s Ex. 4 at 4.

In other words, when swearing out the search warrant to search Mr. Chhipa's house, the FBI asked this Court to believe that it linked the Carl Johnson Facebook account to Mohammed Chhipa because in a conversation the user of that account referred to *part* of a *middle name* and referenced the *entire Northern Virginia area* as the place where he lived.

Of course this is not how the Carl Johnson account was determined to be Mr. Chhipa. It would be impossible to identify someone in this way. The Carl Johnson account was determined to be Mr. Chhipa through prior undisclosed surveillance at least as far back as 2013. *See* Def. Ex. 1. The surveillance or search is presumed to

be warrantless because if it was not, the FBI would have provided the material associated with it, and would not have gone through the trouble of creating the strained, implausible explanation as to how it connected the Carl Johnson Facebook account to Mohammed Chhipa.

Third, just days later, according to a search warrant for nine Facebook accounts:

Def. Ex. 5, *Search Warrant for Nine Facebook Accounts* at 6 (Aug. 8, 2019).

Here, the government's surveillance initiated "observation" of the Carl Johnson account, *and* linked the Carl Johnson account to Mohammed Chhipa. But for these two unlawful events, law enforcement would have had no reason to query a phone number associated with Mr. Chhipa which then led to another Facebook account. Thus, the government "used" material from its surveillance derivatively, even if not as direct evidence against Mr. Chhipa.

The same logic applies to two other Facebook accounts, in which the FBI states:

Id.

Without the covert surveillance that generated the "observation" of the Carl Johnson account, the OCE would not have been observing the [redacted] account. Likewise, for the [redacted] account, but for the surveillance connecting Mohammed Chhipa to the Carl Johnson account, the FBI would have had no reason to issue a grand jury subpoena to Google for all accounts associated with Mohammed Chhipa's phone number.

Fourth, this same search warrant for nine Facebook accounts implies that another Facebook account was discovered on March 28, 2019. It states that the account was "observed," with no indication as to why the FBI would suddenly chose to observe this account. It also makes the farfetched claim that the FBI connected

the dots to Mr. Chhipa through noticing that it began contacting Facebook friends of the Carl Johnson account:

[redacted]

Id.

In reality, the FBI was already aware of this moniker and its connection to Mr. Chhipa from a prior undisclosed surveillance of telegram on an unknown date:

[redacted]

Def. Ex 6, *FBI Electronic Communication* at 2 (July 2, 2019).

Fifth, both search warrants for Mr. Chhipa's residence and nine social media accounts state:

[redacted]

Def.'s Ex. 4 at 5; Def.'s Ex. 5 at 8.

This §2703(d) order for azharc27@gmail.com is for an email address that the government would not have known about based on the information that had been returned from legal processes in the "re-opened" investigation up to that point.

Indeed, when examining the application and order for the §2703(d) request, (Def.'s Ex. 7) it does not even *attempt* to link the email address to Carl Johnson or Mohamad Chhipa. It recites language posted from the Carl Johnson account, states the language is extremist, and then baldly asks for information from a seemingly random email account – with zero connection to "Carl Johnson." The return on that §2703(d) order is a fruit of unlawful surveillance which was then used as probable cause to obtain other fruits.

Fifth and finally, in its August 8, 2019 application for a search warrant for nine Facebook accounts, the FBI relies on prior surveillance to establish probable cause and discover other links and other accounts, stating as part of its probable cause process that "the FBI queried its holdings":

Def. Ex. 5 at 7.

These are just a few examples of "uses" of unlawful surveillance material that the defense was able to identify combing through tens of thousands of heavily redacted documents and being shielded from the substantive material in CIPA process. Without a doubt there are plenty more.

It is unlikely that this Court would like to spend the countless hours and days it would require to reconstruct some of the timelines showing what evidence came from where, tracing it back to its origin. This is where defense counsel's review becomes necessary. Counsel has already done what it can to piece together steps in the investigation, after reviewing mountains of heavily redacted documents produced in no particular order, and certainly not chronological order. This review reveals multiple "uses" of warrantlessly collected material, likely from Section 702 and other convert surveillance programs.

Conclusion

The only way to ensure that Mr. Chhipa's Constitutional rights are properly protected during the effort to strip him of his freedom is to compel disclosure of all the FISA material and all surveillance material used against him and suppress the fruits of the collection.

Respectfully Submitted,
MOHAMMED CHHIPA,
By Counsel
/s/

Jessica N. Carmichael, VSB #78339
Zachary A. Deubler, VSB #90669
CARMICHAEL ELLIS & BROCK, PLLC
108 N. Alfred Street, 1st Floor
Alexandria, VA 22314
703.684.7908 (T)/703.649.6360 (F)
zach@carmichaellegal.com
jessica@carmichaellegal.com

CERTIFICATE OF SERVICE

I hereby certify that on this 16th day of September, 2024, I filed the foregoing pleading through the ECF system, which shall then send an electronic copy of this pleading to all parties in this action.

/s/
Jessica N. Carmichael